


| | | | | | |
|--|--|----------------|------------|----------|---|
| IT STANDARD OPERATING PROCEDURE | DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh | | | |  |
| TITLE: | IT ACCESS CONTROL | | | | |
| SOP No. 1.0.11 | Issue Date | Effective Date | Review Due | Copy No. | Page 1 of 5 |
| | | | | | |

1.0.11 Access Control

PURPOSE

The purpose of this SOP is to define the procedures and guidelines for controlling access to information systems, data, and resources within the organization.

SCOPE

This SOP applies to all employees, contractors, and third-party users who have access to the organization's information systems.

ROLES AND RESPONSIBILITIES

a. IT Security Officer is responsible for:

- Oversee the implementation and enforcement of access control policies.
- Conduct regular access control audits and assessments.
- Ensure alignment of IT initiatives with organizational goals.
- Investigate and respond to access control incidents.

b. Network or System Administrator is responsible for:


- Implement and manage access control mechanisms on systems.
- Grant and revoke access permissions based on role and need.
- Regularly review access logs for anomalies and unauthorized access.

c. IT Support Engineer is responsible for:

- Handle access requests and assist with access-related issues.
- Verify user identity before granting access.
- Escalate access control issues to the IT Security Officer.

ACCESS CONTROL POLICISE

- Clearly define access control policies, including user account creation, modification, and termination procedures.
- Implement the principle of least privilege, granting users the minimum access necessary to perform their duties.
- Define access control levels based on job roles and responsibilities.

| | | | | | |
|--|--|----------------|------------|----------|---|
| IT STANDARD OPERATING PROCEDURE | DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh | | | |  |
| TITLE: | IT ACCESS CONTROL | | | | |
| SOP No. 1.0.11 | Issue Date | Effective Date | Review Due | Copy No. | Page 2 of 5 |
| | | | | | |

USER AUTHENTICATION

- a. Enforce strong password policies, including regular password changes.
- b. Implement multi-factor authentication for sensitive systems and data.
- c. Disable inactive accounts promptly.

USER ACCESS REQUESTS

- a. Users must submit access requests through a standardized form. (Appendix-A)
- b. Access requests must be approved by the user's supervisor or department head.
- c. Requests for elevated privileges require additional approval from the IT Security Manager.

DOCUMENTATION AND RECORD-KEEPING

- 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


PRECAUTIONS

1. ACCESS REVIEW AND AUDITING

- a. IT and Information security team will conduct periodic access reviews to ensure permissions align with current job responsibilities.
- b. Regularly audit access logs for unauthorized access attempts.
- c. Investigate and address any discrepancies or anomalies promptly.

2. ACCESS TERMINATION

- a. Terminate access immediately upon employee termination or role change.
- b. Disabling accounts of employees on extended leave or sabbatical upon discussing with HR.
- c. Conduct exit interviews to remind employees of their responsibility to return company assets and cease unauthorized access.

| | | | | | | |
|--|--|----------------|------------|----------|-------------|---|
| IT STANDARD OPERATING PROCEDURE | DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh | | | | |  |
| TITLE: | IT ACCESS CONTROL | | | | | |
| SOP No. 1.0.11 | Issue Date | Effective Date | Review Due | Copy No. | Page 3 of 5 | |

3. PHYSICAL ACCESS CONTROL

- a. Server Rooms are locked and key is controlled by assigning specific IT persons only.
- b. Restrict physical access to networking equipment and critical infrastructure.

4. INCIDENT RESPONSE

- a. Establish procedures for responding to unauthorized access incidents.
- b. Notify affected parties promptly and take corrective actions.
- c. Document and report access control incidents to management.
(See Reference SOP-1.0.9)

5. TRAINING AND AWARENESS

- a. Provide regular training to employees on access control policies and procedures.
- b. Promote awareness of the importance of access control in safeguarding organizational assets.


6. 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.

7. 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.

8. Accessibility:

| | | | | | | |
|--|--|----------------|------------|----------|-------------|---|
| IT STANDARD OPERATING PROCEDURE | DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh | | | | |  |
| TITLE: | IT ACCESS CONTROL | | | | | |
| SOP No. 1.0.11 | Issue Date | Effective Date | Review Due | Copy No. | Page 4 of 5 | |
| | | | | | | |

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

| SOP No. | SOP Name |
|---------|--------------------------|
| 1.0.9 | Incident Response |
| Policy | IT Access Control Policy |

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 In house

APPENDICES

| | |
|------------|-------------------------|
| APPENDIX-A | User Authorization Form |
| | |
| | |

REVISION HISTORY

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

| | | | | | |
|--|--|----------------|------------|----------|---|
| IT STANDARD OPERATING PROCEDURE | DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh | | | |  |
| TITLE: | IT ACCESS CONTROL | | | | |
| SOP No. 1.0.11 | Issue Date | Effective Date | Review Due | Copy No. | Page 5 of 5 |
| | | | | | |

| | | |
|--------------------------|------------------|-------------|
| 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: <ol style="list-style-type: none"> 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. |
|---|