


STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Access Control Authorization Policy				

Access Control Authorization Policy

Policy Statement:

- a. Clearly articulate the purpose and objectives of the Access Control Policy.
- b. Emphasize the importance of access control in protecting sensitive information and maintaining the organization's security posture.

Scope:

- a. Define the scope of the policy, specifying the systems, data, and personnel to which the policy applies.
- b. Identify any exceptions or specific scenarios not covered by the policy.

Access Control Principles:

Principle of Least Privilege:

- a. Users and systems should have the minimum access necessary to perform their duties.

Need-to-Know Principle:

Access to information is restricted to individuals who need the information for legitimate business purposes.

Separation of Duties:

Ensure that critical tasks are divided among multiple individuals to prevent conflicts of interest and unauthorized activities.

User Authentication:

Password Policy:

Define requirements for strong passwords, including length, complexity, and expiration.

Promote the use of passphrases and discourage password sharing.

Multi-Factor Authentication (MFA):


Mandate the use of MFA for accessing sensitive systems and data.

User Access Management:

User Account Creation:

Establish procedures for creating user accounts, including verification of user identity.

Specify who has the authority to approve new user accounts.

STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT				
	Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Access Control Authorization Policy				

User Account Modification and Termination:

Define the process for modifying user access rights based on role changes.

Outline procedures for promptly terminating access upon employee termination or role change.

Access Control Levels:

Categorize information and systems based on sensitivity and assign access control levels accordingly.

Clearly define access permissions for each level and restrict access to authorized personnel.

Access Requests:

Access Request Procedures:

Specify how users should request access, including the submission process and required information.

Define the approval process, including the roles responsible for granting access.

Elevated Privileges:

Outline procedures for requesting and approving elevated privileges.

Define conditions under which elevated privileges may be granted.

Physical Access Controls:

Implement controls to restrict physical access to critical infrastructure, server rooms, and networking equipment.

Specify who has authorization to enter restricted areas.

Monitoring and Auditing:

Access Logs:

Mandate the logging of access events, including successful and unsuccessful attempts.

Define retention periods for access logs.

Regular Audits:

Conduct periodic access reviews and audits to ensure compliance with access control policies.


Investigate and address any discrepancies or anomalies.

Incident Response:

Establish procedures for responding to unauthorized access incidents.

Define reporting mechanisms and escalation procedures for suspected or confirmed incidents.

Specify actions to be taken to mitigate and remediate access control breaches.

STANDARD OPERATING PROCEDURE	DBLGROUP IT DEPARTMENT				
	Capita South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh				
TITLE:	Access Control Authorization Policy				

Training and Awareness:

Provide regular training to employees on access control policies and procedures.

Emphasize the importance of responsible use of access privileges and reporting any suspicious activities.

Compliance:

Ensure that the access control policies align with relevant laws, regulations, and industry standards.

Conduct periodic assessments to verify adherence to access control policies.

Review and Revision:

Establish a regular review schedule to update the policy based on changes in technology, organizational structure, or security requirements.

Specify the roles responsible for policy review and approval.

Documentation and Record-keeping:

Maintain detailed records of access requests, approvals, modifications, and terminations.

Keep an inventory of users with access to sensitive systems and data.

Enforcement and Consequences:

Clearly communicate the consequences of violating access control policies.

Outline disciplinary actions for non-compliance.