

Access Control and Permission Management Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Version:1.2

Version History

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	28/6/2022	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.1	28/6/2023	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.2	28/7/2024	P.Sahoo	Shankar VRG	Amit Sobti	Reviewed

1. Purpose

The purpose of this Access Control and Permission Management Policy is to define the organization's framework for controlling access to systems, applications, and data. The goal is to ensure that sensitive information is only accessible to authorized personnel based on their roles and responsibilities, thus maintaining the confidentiality, integrity, and availability of organizational resources.

2. Scope

This policy applies to all users who have access to the organization's information systems, including employees, contractors, third-party vendors, and any other external entities who are granted access. It covers all organizational data, applications, systems, network devices, and physical access points that require access control.

3. Policy Statement

The organization will implement and enforce access control mechanisms to ensure:

- Access is granted based on the principle of least privilege, meaning users are only provided with the minimum access required to perform their job functions.
- Access to sensitive or critical systems and data is controlled and monitored to prevent unauthorized use or data breaches.
- User access rights are reviewed and updated regularly to ensure compliance with organizational needs and security requirements.

4. User Authentication and Authorization

- **Authentication Requirements:**
 - All users must authenticate using strong methods. At a minimum, authentication should require a username and password, and multi-factor authentication (MFA) should be enforced for accessing sensitive systems or data.
 - Password policies should require complexity (minimum length, use of special characters, etc.) and periodic changes.
- **Authorization Process:**

- Authorization will be granted based on roles and responsibilities or other applicable access control models. After authentication, users will be granted access to resources based on predefined rules that match their job requirements.
- Access rights must be documented and reviewed to ensure users only have access to what they need to perform their job functions.

5. Access Control Principles

- **Least Privilege:**

- Users will be granted only the minimum level of access required for them to perform their job duties. Access to sensitive data or systems will be restricted to users with specific job-related needs.

- **Need-to-Know:**

- Access to sensitive information or systems will be granted based on a user's need to know. Users will only be able to access data relevant to their tasks, and unnecessary or excessive access rights will be denied.

- **Separation of Duties:**

- No individual should have access to critical systems that would allow them to perform conflicting actions (e.g., authorizing payments and approving transactions). Responsibilities should be divided to minimize risk and prevent fraud.

- **Temporary Access:**

- If users require temporary access to resources, permissions will be granted for a limited time and will be automatically revoked after the access period expires. This applies to contractors, temporary employees, and external vendors.

6. Access Request and Approval Process

- **Access Request:**

- Users must submit an access request through an authorized channel, such as a centralized system or helpdesk, providing details such as the required resources, justification, and duration for access.

- **Access Approval:**

- Access requests will be reviewed and approved by the relevant authority, such as the user's manager, system owner, or information security team.
- For high-risk or sensitive resources, approval should involve multiple levels of authorization or a security officer's oversight.

7. Permission Management

- **Assigning Permissions:**

- Permissions will be assigned based on the user's job role and access requirements. Systems must be configured to enforce role-based permissions and restrict access where necessary.
- Permissions should include read, write, execute, or delete rights based on the principle of least privilege.

8. Logging and Monitoring Access

- **Logging:**

- All access events should be logged, including successful and failed login attempts, access to sensitive resources, and changes to user permissions.
- Logs should include information about the user, time of access, IP address, and actions performed.

- **Monitoring:**

- Logs should be continuously monitored for unusual access patterns or potential security breaches, such as unauthorized access attempts or changes to access rights.
- Automated alerts should be configured to notify the security team of potential violations, such as abnormal login times or access from unapproved locations.