Standard Operating Procedure (SOP): Access Authorization and User Permissions Management

This SOP details the process of **access authorization and user permissions management**, encompassing the assignment, review, and revocation of user access rights to systems and data. It ensures that only authorized personnel have appropriate permissions, incorporating principles of least privilege, role-based access control, periodic access reviews, and secure onboarding and offboarding procedures. The goal is to protect sensitive information, maintain compliance with security policies, and minimize risk of unauthorized access.

1. Purpose

To establish a standard process for granting, reviewing, modifying, and revoking access to information systems and data, ensuring compliance with security policies and regulatory requirements.

2. Scope

This SOP applies to all personnel requiring access to organizational IT systems, applications, networks, and data, including employees, contractors, and third parties.

3. Roles & Responsibilities

Role	Responsibility
System Owner	Defines access requirements, approves access requests, and ensures periodic review of user permissions.
IT Administrator	Implements, modifies, and revokes access rights as authorized.
HR Department	Informs IT/Admin regarding employee onboarding, transfers, and terminations.
User	Uses granted access responsibly and reports any unauthorized access.
Compliance Officer	Oversees audit and regulatory compliance for access management.

4. Procedures

4.1 Access Request & Authorization

1. User or manager submits an access request form specifying justification and required permissions.
2. System Owner reviews and approves/rejects the request based on role requirements and least privilege principles.
3. IT Administrator provision access as per approved request, documenting all actions taken.

4.2 Role-Based Access Control

- Assign users to pre-defined roles aligned with job functions.
- Limit permissions at role level to reduce risk and ensure consistency.
- Periodic review of roles to ensure alignment with organizational needs.

4.3 Periodic Access Review

1. Conduct access reviews at least quarterly or as required by policy.
2. System Owners and Compliance Officer review user access lists and permissions.
3. Identify and remediate excessive, outdated, or unauthorized permissions.
4. Document findings and actions taken.

4.4 Onboarding and Offboarding

- **Onboarding:** HR notifies IT/Admin of new hires. Access is provisioned based on the approved role and documented accordingly.
- **Offboarding:** HR notifies IT/Admin of terminations or transfers. All access privileges are revoked promptly on the last working day or role change.

- Retrieve or disable physical and logical credentials (e.g., badges, tokens, passwords).

4.5 Access Modification

- Managers submit modification requests when user roles or responsibilities change.
- Review and approve modifications following the access request process.
- Update user permissions and document changes.

5. Documentation & Audit

- Maintain records of all access requests, approvals, permissions, and revocations.
- Ensure logs are auditable and available for compliance verification.
- Report and escalate any unauthorized access attempts or incidents.

6. Review & Maintenance

This SOP shall be reviewed annually or following significant changes to systems, processes, or regulatory requirements.

7. Related Policies & References

- Information Security Policy
- Data Protection Policy
- Regulatory Compliance Requirements (e.g., GDPR, HIPAA)

8. Revision History

Version	Date	Description	Author
1.0	2024-06-18	Initial version	[Your Name]