

User Access Management Manual Template for Enterprise Applications

1. Purpose

This User Access Management Manual provides guidelines for managing user access to enterprise applications in order to ensure information security, compliance, and standardized access controls.

2. Scope

This manual applies to all users, administrators, and managers who require or manage access to enterprise applications within the organization.

3. Roles and Responsibilities

Role	Responsibility
User	Requests access, uses applications as per assigned permissions, reports access issues.
Manager	Authorizes access requests, reviews and approves access levels for users under their supervision.
System Administrator	Implements access permissions, maintains user data, reviews access logs, and manages revocation.
IT Security	Monitors access control compliance and conducts periodic audits.

4. Access Management Procedures

4.1 Access Request

1. User completes and submits the Access Request Form to their manager.
2. Manager reviews and forwards approved request to the system administrator.
3. System administrator reviews and processes the access request.
4. User is notified upon access provisioning or denial.

4.2 Access Review

- Managers review user access on a quarterly basis.
- System administrators generate and distribute access reports for validation.
- Irrelevant or redundant access rights are revoked as required.

4.3 Access Revocation

1. Access is revoked immediately upon role change, termination, or transfer.
2. Managers notify system administrators of any user status changes.
3. System administrator removes or adjusts user permissions accordingly.

5. Access Levels

Access Level	Description
End User	Standard access to application features required for daily responsibilities.
Power User	Enhanced access for advanced functionalities, subject to approval.
Administrator	Full control for application configuration and user management.

6. Review and Audit

- Access controls are to be reviewed quarterly by IT Security.
- Audit logs must be maintained and reviewed for unauthorized access attempts.

7. Contact Information

For questions or support regarding user access, please contact the IT Helpdesk at *your-it-helpdesk@company.com*.