APPROVED

Approver
2026-01-30 00:55:07

SOP-002 v1.0 – User Management and Access Control for VDC

Document ID: SOP-002

Title: User Management and Access Control for VDCVersion: v1.0

Effective Date: Jam 28th 2026

Owner: William OConnell

rApproved By: Jane Smith

1. Purpose

To define the process for granting, modifying, and revoking user access to the VDC system, ensuring appropriate segregation of duties, least privilege, and compliance with 21 CFR Part 11.

2. Scope

This SOP applies to all human users and service accounts that access VDC at `https://williamoconnellpmp.com` in non-development environments (test, staging, production).

3. Definitions

- Submitter: User who uploads and submits documents for approval.
- Approver: User who reviews and approves or rejects submitted documents.
- System Administrator (SysAdmin): User with elevated privileges to configure the system and manage accounts; may not approve documents they administer.
- Read-Only User: User who may view documents and audit trails but cannot initiate workflow actions.

4. Roles and Permissions

- Submitter
  - Create and edit draft documents.
  - Submit documents into workflow.
  - View their own submissions and associated audit trails.
- Approver
  - View and review documents assigned for approval.
  - Approve or reject submissions with comments.
- System Admin
  - Manage user accounts and roles.
  - Configure non-GxP-critical application parameters.

    - Cannot alter historical audit records or documents.
- Read-Only
    - View documents, metadata, and audit trails.
    - No ability to upload, edit, or approve.

Role permissions are defined and maintained in VDC configuration and, where applicable, in Cognito groups or equivalent identity platform groups.

5. Access Request and Approval

5.1 Request Initiation

- Line manager or equivalent initiates access request via approved mechanism (form, ticketing system, or controlled email template).
- Request includes:
    - User name and corporate email.
    - Business justification.
    - Requested role(s) and environment(s).

5.2 Approval

- System Owner (or delegate) and QA review and approve or reject the request.
- Approvals must be documented (signature, electronic approval, or ticket action log).

6. Account Provisioning

- Upon approval, SysAdmin:
    - Creates or enables the user in the identity provider (e.g., Cognito).
    - Assigns the approved role(s) by mapping to appropriate groups.
    - Confirms that multi-factor authentication is enforced where configured.
- SysAdmin records in the Access Register:
    - User identifier, roles, date provisioned, approver(s), and environment(s).

7. Role Changes

- Role upgrade or downgrade follows the same approval process as new access.
- SysAdmin updates group membership and logs:
    - Previous role(s), new role(s), date, and approver.

8. Account Deactivation

- Access must be deactivated when:
    - Employment or contract ends.
    - Role no longer requires system access.

  - User has been inactive beyond the defined threshold, if enforced.
- SysAdmin disables login capability and removes role assignments within the defined timeframe (e.g., 1 business day) after notification.
- Deactivation is recorded in the Access Register, with reason and date.

9. Periodic Access Review

- At least annually, System Owner and QA:
  - Export or review list of active users and their roles.
  - Confirm each user’s continued need for access and appropriate role.
- Discrepancies (e.g., excessive privilege, orphaned accounts) are corrected and documented, and may trigger CAPA per SOP-005.

10. Training Requirement

- Users must complete role-appropriate training and sign training records per SOP-006 before being granted production access.

11. References

- SOP-001 VDC System Governance and Validation.
- SOP-005 Incident, Deviation, and CAPA Management.
- SOP-006 Training and Qualification.