

SOP Template: Workstation Setup and Access Provisioning

This SOP details the process of **workstation setup and access provisioning**, including hardware and software configuration, user account creation, access rights assignment, security protocol implementation, and system validation. The aim is to ensure efficient and secure workstation readiness for new and existing users, facilitating smooth operational workflows and protecting organizational data integrity.

1. Purpose

To establish a standardized procedure for setting up user workstations and provisioning appropriate access to systems and applications, ensuring consistency, security, and operational efficiency.

2. Scope

This SOP applies to IT personnel responsible for provisioning, configuring, and validating workstations for all organizational users, including new hires and existing staff requiring access changes.

3. Responsibilities

- **IT Support:** Executes setup, configuration, and provisioning.
- **HR/Managers:** Submits user access requests and approvals.
- **End Users:** Verifies workstation access and reports any issues.

4. Procedure

1. Request Initiation

- Manager/HR fills and submits user access request form with user details and required access.

2. Hardware Preparation

- Assign or procure workstation hardware (PC/laptop, monitor, peripherals).
- Physically inspect hardware for defects.
- Label hardware as per asset management policy.

3. Operating System Installation & Configuration

- Install approved OS (e.g., Windows, macOS, Linux).
- Apply latest OS updates and security patches.
- Set system hostname and network configuration.

4. Software Installation

- Install standard office productivity suite and security software.
- Install additional approved applications per user role.

5. User Account Creation

- Create user account in Active Directory/LDAP or relevant directory service.
- Assign username and temporary password.

6. Access Rights Assignment

- Grant access to shared drives, folders, email, and required applications per access request.
- Assign user to appropriate groups/roles.

7. Security Protocol Implementation

- Configure local security policies (e.g., password complexity, screen lock, firewall).
- Enable disk encryption and endpoint protection.
- Apply necessary restrictions (admin privileges, software installation permissions).

8. System Validation & Handover

- Test user login and verify all applications and network resources are accessible.
- Document setup details and have user sign off on system acceptance.

9. Documentation & Support
- Update asset management and access records.
 - Provide user with basic usage and security guidelines.
 - Log setup completion in the ticketing system.

5. Documentation

Document/Record	Responsible	Retention
User Access Request Form	HR/Manager	As per HR policy
Asset Register	IT Support	Workstation life cycle
Access Log/Provisioning Record	IT Support	Minimum 1 year

6. References

- IT Security Policy
- Acceptable Use Policy
- Asset Management Policy

7. Revision History

Version	Date	Author	Description
1.0	2024-06-10	IT Department	Initial SOP release

Note: Customize this template per your organization's systems, tools, and regulatory requirements.