Software Deployment SOP

Purpose

To define a standardized procedure for deploying new software or migrating existing systems, including licensing, installation, staff communication, training, and compliance. This ensures security, operational continuity, and user readiness. This SOP applies to all new software deployments and upgrades, including organization-wide platforms, department-specific tools, and licensed applications.

1. Procedure
2. New software must be requested via the IT Account Request Form. This requires approval from the department head.
3. IT assesses compatibility, security risks, licensing models, integration needs, and long-term support. Budget and compliance requirements are reviewed by Fiscal and HR/Legal.
4. Develop a staff communication plan:

* For major deployments, notify all impacted staff at least 90 days in advance. Use emails, staff meetings, and internal memos.
* Establish monthly reminders up to deployments and weekly reminders in the final 30 days.
* Designate IT staff for questions and clarifications.

1. Licensing and procurement:

* Purchase licenses from approved vendors (see IT Procurement SOP).
* Record license details, expiration dates, and usage limits in the license tracking system.
* Maintain license keys in a secure, access-controlled location.

1. Installation and rollout:

* During the pilot phase, test deployment with 3-5 users across departments. Log bugs, compatibility issues, and user feedback.
* During full rollout, schedule installation dates by team or department. Use automated scripts or endpoint management tools for standardized deployment.
* Link user accounts and set permissions based on roles.
* Disable or remove previous conflicting software where applicable.

1. Provide multilingual training during rollout period. Deliver live or recorded sessions, user guides, and FAQs. Require staff to complete onboarding modules for critical applications.
2. Offer 24/7 post-deployment support for up to two weeks via ticketing system, emergency contact channel, and in-person walk-in hours.
3. Conduct license audits quarterly to ensure usage remains within limits.
4. Monitor software usage and update status via InvGate. Flag non-compliant devices or accounts for review.
5. Ensure data retention and transfer policies are followed during migrations.
6. Schedule regular update checks based on vendor release cycles. Test critical patches before deployment. Document patch deployment in ticketing system and asset logs.
7. Within 30 days of deployment, conduct a feedback survey, hold a debrief with IT and department leads, review incident logs and training gaps, and update relevant SOPs, if needed.

This SOP should be reviewed annually or upon major platform changes.