Unpaid Tools, Services, and Software Usage SOP

Purpose

To establish a standardized process for reviewing, approving, and managing the use of unpaid or free software, tools, or services that access or interact with organization data or are used in organization operations. This ensures security, compliance, data integrity, and minimizes operational risks. This SOP applies to all staff, interns, and contractors using or requesting unpaid software, web tools, cloud services, or any technology that accesses, stores, transmits, or processes organizational data or is used in the context of work.

1. All staff must submit an Account Request Form before using any free software or service. The form should include tool/service name and link, purpose of use, data involved, access or account requirements, and duration or frequency of use.
2. IT reviews the tools for data access and privacy policy, security risks, integration with existing systems, and compliance with HIPAA, FERPA, and the Sensitive Data Policy. If unclear, IT may conduct a risk assessment or vendor due diligence and test the tools in a controlled environment.
3. For low-risk tools (no access to sensitive data or installation required), may be approved by IT Lead alone. For medium/high-risk tools (handling sensitive data or requiring account integration), require sign-off from IT Lead and HR. IT documents approval status and rationale in the internal tracking system.
4. Approved tools must be used only through official organizational accounts, must follow data handling policies, and are subject to periodic IT audit and review.
5. IT provides setup guidance if necessary and records tool usage in the IT asset or software inventory system.
6. IT reserves the right to restrict or revoke access if a tool poses newly identified risks, the tool’s privacy policy changes unfavorably, or staff misuse the service (see Misue of Device SOP).
7. IT reviews all active unpaid services quarterly. Decommission any tool that is no longer in use or does not meet current standards.
8. Any use of unapproved tools will be considered a policy violation and handled per disciplinary protocols.

This SOP should be reviewed annually or after significant changes in the data policy, IT infrastructure, or legal compliance requirements.