# Training Plan: Approved Tools, Acceptable Use Policies, and Shadow IT Awareness

## 1. Objective

To educate all staff on the secure and responsible use of organizational tools, reinforce compliance with acceptable use policies, and raise awareness about the risks and consequences of using unauthorized systems (shadow IT), thereby strengthening the organization’s cybersecurity posture.

## 2. Target Audience

* All full-time and part-time employees
* Contractors and third-party service providers with system access
* New hires (as part of onboarding)

## 3. Training Frequency and Format

|  |  |  |  |
| --- | --- | --- | --- |
| Session Type | Frequency | Format | Duration |
| Core Training | Quarterly | In-person or virtual | 1 hour |
| Refresher Session | Bi-annually | Online (self-paced) | 30 mins |
| Department-Specific Clinics | As needed | Onsite or virtual | 45 mins |
| New Hire Orientation | Upon joining | Classroom/Online | 1 hour |

## 4. Key Learning Modules

### Module 1: Approved Tools and Platforms

* Definition of "approved tools" in the organization
* Tool lifecycle: from procurement to decommissioning
* Examples of sanctioned communication, storage, and productivity tools
* How to request access to tools or suggest new ones

**Outcome**: Employees understand what tools are authorized and why tool compliance matters.

### Module 2: Acceptable Use Policy (AUP)

* Overview of organizational AUP
* Dos and Don’ts when accessing corporate systems, emails, and internet resources
* Use of personal devices and remote access guidelines (BYOD policy)
* Real-world case studies on AUP violations and consequences

**Outcome**: Employees become fully aware of behaviour expected when using IT resources.

### Module 3: Shadow IT – Risks and Impact

* What is shadow IT, and why do employees turn to it?
* Data leakage, compliance breaches, and security gaps caused by unauthorized apps
* How shadow IT can compromise system integrity and incident response
* Encouraging transparent communication when needs are unmet by current tools

**Outcome**: Participants recognize the hidden dangers of unapproved tech and feel empowered to act responsibly.

### 5. Training Delivery Methods

* **Live Workshops** - Led by IT and compliance teams with Q&A
* **Interactive eLearning Modules** - With real-life scenarios and gamified quizzes
* **Infographics and Job Aids** - Placed on internal communication boards
* **Short Videos (2-3 minutes)** - Covering tool-specific guidance
* **Feedback Forms** - Post-training evaluations to adjust future sessions

### 6. Evaluation and Metrics

|  |  |
| --- | --- |
| Metric | Measurement Method |
| Training Completion Rate | LMS tracking and attendance |
| Policy Acknowledgement Rate | Signed AUP forms |
| Incidents Related to Shadow IT | IT helpdesk and audit logs |
| Requests for New Tool Evaluation | Monthly IT governance reports |
| Post-Training Knowledge Retention | Quizzes and follow-up surveys |

## 7. Roles and Responsibilities

* **IT Department** - Develop technical content, approve training material
* **Compliance/HR** - Ensure policy alignment and recordkeeping
* **Line Managers** - Reinforce lessons within teams, monitor adherence
* **Employees** - Engage in training and report suspected shadow IT

## 8. Continuous Improvement Plan

* Conduct annual training content reviews to reflect tool updates and emerging risks
* Use anonymized incident data to refine training modules
* Collect ongoing employee feedback to ensure relevance and engagement
* Include shadow IT discussions in monthly security newsletters