



FedRAMP Moderate Templates

Awareness and Training Family Implementation Checklist

Policy and Documentation (AT-1)

- ☐ Develop and document awareness and training policy at organization, mission/business process, and/or system levels
- ☐ Create procedures for implementing awareness and training policy and controls
- ☐ Designate an official to manage awareness and training policy and procedures
- ☐ Review and update policy at least every 3 years and after organization-defined events
- ☐ Review and update procedures at least annually and after significant changes
- ☐ Disseminate policy and procedures to relevant personnel

Security and Privacy Literacy Training (AT-2)

- ☐ Provide security and privacy literacy training to all system users (managers, senior executives, contractors)
- ☐ Deliver initial training to all new users before granting system access
- ☐ Conduct literacy training at least annually for all users
- ☐ Provide training when required by system changes
- ☐ Provide training following organization-defined significant events
- ☐ Implement organization-defined awareness techniques to increase security and privacy awareness
- ☐ Update literacy training and awareness content at least annually
- ☐ Update training content following organization-defined events
- ☐ Incorporate lessons learned from internal or external security incidents into training
- ☐ Incorporate lessons learned from security breaches into awareness techniques

Literacy Training Enhancements

- ☐ **AT-2(2):** Provide training on recognizing potential indicators of insider threats
- ☐ **AT-2(2):** Provide training on reporting potential indicators of insider threats



FedRAMP Moderate Templates

- ☐ **AT-2(3):** Provide training on recognizing social engineering attempts
- ☐ **AT-2(3):** Provide training on recognizing social mining attempts
- ☐ **AT-2(3):** Provide training on reporting social engineering and social mining incidents

Role-Based Security and Privacy Training (AT-3)

- ☐ Identify all roles and responsibilities requiring specialized security training
- ☐ Develop role-based training content for each identified role
- ☐ Provide role-based training before authorizing access to systems or information
- ☐ Provide role-based training before personnel perform assigned duties
- ☐ Conduct role-based training at least annually for all personnel with defined roles
- ☐ Provide additional training when required by system changes
- ☐ Update role-based training content at least annually
- ☐ Update role-based training following organization-defined events
- ☐ Incorporate lessons learned from security incidents into role-based training
- ☐ Incorporate lessons learned from security breaches into role-based training

Training Records (AT-4)

- ☐ Document all information security training activities
- ☐ Document all privacy training activities
- ☐ Document security and privacy awareness training completion
- ☐ Document role-based security and privacy training completion
- ☐ Monitor training activities to ensure compliance
- ☐ Retain individual training records for at least one (1) year after training completion
- ☐ Establish system for tracking training completion and currency
- ☐ Maintain records accessible for audit and compliance verification

Key Timeframes to Remember

- **Policy reviews:** Every 3 years minimum
- **Procedure reviews:** Annually minimum
- **Literacy training:** Annually for all users
- **Role-based training:** Annually for all personnel with security roles



FedRAMP Moderate Templates

- **Content updates:** Annually minimum
- **Training record retention:** At least 1 year after completion